

Forum: [Hack Forums](#)

Thread: [Getting window title from PEB](#)

ShallowME - April 6, 2020, 6:44 pm

Getting window title from PEB.

So I got the address of the PEB using NtQuerySystemInformation.

PEB + 0x10 => ProcessParameters

ProcessParameters + 0x70 => WindowTitle

I typecast this address to `_UNICODE_STRING` structure but still I get my Buffer as NULL.
What gives?

4Txe4y33C9zvNhMj - April 7, 2020, 2:13 am

Why not just use `GetWindowText()`?

The info is also stored in a `_LARGE_UNICODE_STRING` structure.

Check this out:

<https://www.nccgroup.trust/globalassets/newsroom/uk/blog/documents/2015/07/exploiting-cve-2015.pdf>

Should be on page 13.

ShallowME - April 7, 2020, 2:46 am

(Apr 7, 2020 02:13 AM)4Txe4y33C9zvNhMj Wrote: [\[CITE\]](#) Why not just use `GetWindowText()`?

The info is also stored in a `_LARGE_UNICODE_STRING` structure.

Check this out:

<https://www.nccgroup.trust/globalassets/newsroom/uk/blog/documents/2015/07/exploiting-cve-2015.pdf>

Should be on page 13. This is supposed to be an exercise. I don't want to use `GetWindowText`.

4Txe4y33C9zvNhMj - April 7, 2020, 2:49 am

(Apr 7, 2020 02:46 AM)ShallowME Wrote: [\[CITE\]](#) This is supposed to be an exercise. I don't want to use `GetWindowText`.

Did you read the link I sent you?

Describes how to get the string you need from the PEB.

ShallowME - April 7, 2020, 6:12 am

(Apr 7, 2020 02:49 AM)4Txe4y33C9zvNhMj Wrote: [\[CITE\]](#) Did you read the link I sent you?

Describes how to get the string you need from the PEB.

Yes, I did. I can do it from WinDbg but for some reason it comes out to be NULL when I do it from

```
Code int main(){
DWORD *PEB_ADDR = NULL;
```

```
__asm{
MOV EAX, FS:[30h]
MOV PEB_ADDR, EAX
}
```

```
void *PebPtr = (void*)PEB_ADDR;
```

```
PebPtr += 0x10;
PebPtr +=0x70;
_UNICODE_STRING *str = (_UNICODE_STRING*)PebPtr;
printf(L"%ws\n",PebPtr->Buffer);
return 0;
}
```

HFDone - April 7, 2020, 6:33 am

PEB + 0x10 => ProcessParameters

??? PebPtr +=0x38; ???

ProcessParameters + 0x70 => WindowTitle

ShallowME - April 7, 2020, 8:46 am

(Apr 7, 2020 06:33 AM)HFDone Wrote: [\[CITE\]](#) PEB + 0x10 => ProcessParameters

??? PebPtr +=0x38; ???

ProcessParameters + 0x70 => WindowTitle

Typo. ??

HFDone - April 7, 2020, 10:42 am

in your code you add to ProcessParameters 0x38 when it shold be 0x70

and you trying to get WindowTitle of console application which is nul

you need to do it with window application

ShallowME - April 7, 2020, 11:48 am

I am doing it for Window's form application.

akali - April 8, 2020, 2:33 am

I don't know which compiler you're using, regardless I'm pretty sure this is wrong.

Code void *PebPtr = (void*)PEB_ADDR;

```
PebPtr += 0x10;
```

```
PebPtr +=0x70;
```

ShallowME - April 8, 2020, 4:02 am

(Apr 8, 2020 02:33 AM)akali Wrote: [\[CITE\]](#) I don't know which compiler you're using, regardless I'm pretty sure this is wrong.

Code void *PebPtr = (void*)PEB_ADDR;

```
PebPtr += 0x10;
```

```
PebPtr +=0x70;
```

I am using GCC.

Why is it wrong? I am type casting it to void so that it doesn't multiply it with sizeof(data_type) when doing pointer arithmetic.

akali - April 8, 2020, 11:48 am

(Apr 8, 2020 04:02 AM)ShallowME Wrote: [\[CITE\]](#) I am using GCC.

Why is it wrong? I am type casting it to void so that it doesn't multiply it with sizeof(data_type) when doing pointer arithmetic.

I guess GCC allows pointer arithmetic to void* types. Microsoft's compiler doesn't. That's why I asked.

ShallowME - April 9, 2020, 6:49 am

(Apr 8, 2020 11:48 AM)akali Wrote: [\[CITE\]](#) I guess GCC allows pointer arithmetic to void* types. Microsoft's compiler doesn't. That's why I asked.

The ASM part is according to MSVC but I have added that here for readability.